UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

UNITED STATES OF AMERICA	§	
	§	
VS.	§	CRIMINAL ACTION NO. 4:15-CR-00467
	§	
LOUIS CLIFFORD SMITH	§	

OPINION AND ORDER

Pending before the Court in the above-referenced cause is Defendant Louis Clifford Smith, Jr.'s ("Smith") Motion to Suppress Evidence Under Seal. Doc. 35. The United States ("Government") has filed a response, Doc. 36, and the parties appeared before the Court on September 14, 2016, to argue their respective positions. After considering the motion, response, oral arguments, and relevant case law, the Court is of the opinion that Defendant's motion should be denied.

I. Background

In 2015, government agents from a number of United States and foreign agencies were involved in an international investigation of child-pornography websites known as "Operation Pacifier." Doc. 35 at 1. These websites operated on the "dark web"—a small part of the world wide web that requires special software to access. *Dark Web*, Wikipedia.org, https://en.wikipedia.org/wiki/Dark_web (last visited Sept. 16, 2017). Not only does dark web access require special software, but unlike websites on the normal web, many dark websites are "hidden," meaning they have not been indexed and, therefore, can only be accessed if the address of the website is known to the user. *See* Docs. 35-2 at 14, 36 at 4. The site at issue in this case, "Playpen" was one such site. Docs. 35-2 at 14, 16, 36 at 4.

Playpen operated on an anonymity network available to Internet users known as "The

Onion Router" or "TOR" network. Docs. 35-2 at 14, 36 at 4. The main advantage of TOR is that it protects users' privacy online by masking the user's Internet Protocol ("IP") address. Docs. 35-2 at 15, 36 at 3–4. It does this by bouncing the user's communications around a worldwide distributed network of relay computers run by volunteers. Docs. 35-2 at 15, 36 at 4. As a result of the anonymity promised by this technique, the dark web is a haven of criminal activity and discerning the identities of individuals engaging in illicit behavior presents a particular challenge to criminal investigators. *See* Docs. 35-2 at 27.

During the course of the Operation Pacifier investigation, FBI agents determined that the computer server that hosted Playpen was located at a web-hosting facility in North Carolina. Docs. 35 at 2, 36 at 5. In February 2015, agents apprehended the site administrator and seized control of Playpen. Docs. 35 at 2, 36 at 5. However, in an effort to determine the identities of—and apprehend—Playpen's users, the FBI chose to continue to operate the website from a government facility in the Eastern District of Virginia from February 20, 2015, until March 4, 2015. Docs. 35 at 2, 36 at 5. In order to effectuate this plan, on February 19, 2015, the FBI sought—and obtained—a warrant from a magistrate judge in the Eastern District of Virginia to deploy a Network Investigative Technique ("NIT") on the website to "investigate any user or administrator who logs into [Playpen] by entering a username and password." Docs. 35-2 at 28.

In the normal course of operation, websites send content to visitors. *Id.* When a user visits a website, the user's computer downloads that website's content and uses it to display web pages on the user's computer. *Id.* The NIT authorized by the magistrate judge in this case was designed to simply augment these normal instructions by sending additional instructions to the user's computer once the user downloaded content. *Id.* These additional instructions would then cause the user's computer to transmit certain identifying information, including the user's IP address,

to a computer controlled by the government. *Id.*

Once the NIT was authorized by the magistrate judge, it was loaded onto the server within the Eastern District of Virginia. Doc. 36 at 8. The Playpen website continued to function normally, and the NIT was undetectable to users of Playpen. *See* Docs. 35 at 2, 26 at 8. However, once a user logged into Playpen to access its pornographic content, the NIT would "attach" and "follow" the user's computer signals back through the dark web's maze, ultimately allowing government agents to pinpoint the user's exact location using the disclosed IP address. Docs. 35-2 at 30, 36 at 8.

Using the NIT, the FBI identified an IP address associated with Playpen user "clitnocker" who had logged into the site and accessed files containing images of a prepubescent girl masturbating and exposing her genitals to the camera and an adult hand spreading open a child's vagina for the camera. Doc. 35 at 5–6. After determining the location of Defendant's computer using the information obtained by the NIT, on July 27, 2015, government agents sought a warrant in the Southern District of Texas to search Defendant's computer. *Id.* at 3. On July 31, 2015, Magistrate Judge John R. Froescher granted this request. *Id.* In a post-*Miranda* interview, Defendant admitted that he had downloaded and viewed child pornography from the Internet. Doc. 36 at 6. The Government's subsequent search of Defendant's computers and hard drives revealed over 270,000 images and over 5,000 videos of young children engaged in sexually explicit conduct. *Id.*

II. Defendant's Motion to Suppress

Defendant now seeks "to suppress all evidence obtained from the Government's illegal search of his computer through the deployment of a 'Network Investigative Technique.'" Doc. 35 at 1. Defendant argues that the search was illegal because it violated (1) Fed. R. Crim. P. 41;

(2) the Federal Magistrates Act, 28 U.S.C. § 636(a); and (3) the Fourth Amendment to the U.S. Constitution. *Id.* Specifically, Defendant contends that the warrant violated Rule 41 because it was "a borderless dragnet search with no geographic limitation." *Id.* at 4.

The Government responds that the search was authorized under subsections (b)(1), (b)(2), and (b)(4) of Rule 41, does not violate the Federal Magistrates Act, and—even if the search did not fit within the letter of Rule 41(b)—"the use of the NIT would nevertheless be reasonable under the Fourth Amendment." Doc. 36 at 7–15. Moreover, even if the warrant was deficient, the Government urges that the good-faith exception to the Fourth Amendment bars suppression. *Id.* at 15–17.

III. Analysis

a. Applicability of Fourth Amendment

Although the Government does briefly argue that a defendant does not have a reasonable expectation of privacy in an IP address, it does so only in making its argument that the search was minimally invasive as required to apply the exigent-circumstances exception to the Fourth Amendment's requirements for obtaining a valid warrant. *See* Doc. 36 at 12. It does not use this as the foundation for an argument that no warrant was necessary because there was no Fourth Amendment search. *See id.* Notwithstanding the Government's failure to make this argument, a number of our sister district courts have proceeded to address this issue *sua sponte* when ruling on motions to suppress in response to the Playpen NIT, noting that "[i]f the use of the NIT was not a search, the Fourth Amendment was not implicated, no warrant was required, and any violation of Rule 41(b) irrelevant." *United States v. Darby*, 2:16CR36, 2016 WL 3189703, at *4 (E.D. Va. June 3, 2016) (citing *Kyllo v. United States*, 533 U.S. 27, 31 (2001)). In doing so, these courts have looked to their respective circuit court's pronouncements on whether a defendant has

a reasonable expectation of privacy in an IP address. Not surprisingly, however, different courts have come to different conclusions about whether the deployment of the NIT constituted a Fourth Amendment search. *Compare, e.g.*, *id.*, at *6 (concluding that deployment of NIT was a search), *and United States v. Ammons*, 3:16-CR-00011-TBR-DW, 2016 WL 4926438, at *3 (W.D. Ky. Sept. 14, 2016) (same), *with, e.g.*, *United States v. Jean*, 5:15-CR-50087-001, 2016 WL 4771096, at *9 (W.D. Ark. Sept. 13, 2016) (concluding that deployment of NIT was likely not a search), *and United States v. Acevedo-Lemus,* SACR 15-00137-CJC, 2016 WL 4208436, at *6 (C.D. Cal. Aug. 8, 2016) (concluding that deployment of NIT was not a search). Because the parties here do not press this issue and neither the Fifth Circuit nor Supreme Court has addressed it, the Court declines to join the fray and will instead proceed on the parties' mutual premise—that the Government's deployment of the NIT was a search under the Fourth Amendment.

b. Fourth Amendment

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

In light of this language, the Supreme Court has imputed two Fourth Amendment requirements to searches and seizures: (1) all searches and seizures must be reasonable; and (2) a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity. *Kentucky v. King*, 563 U.S. 452, 459 (2011) (citing *Payton v. New York*, 445 U.S. 573, 584 (1980)). Accordingly, "a warrant must generally be secured" before executing a search. *Id.* Nevertheless, "[b]ecause the Fourth Amendment's ultimate touchstone is 'reasonableness,' the warrant requirement is subject to certain exceptions." *Brigham City v.*

Stuart, 547 U.S. 398 (2006).

Defendant argues that the search violated the Fourth Amendment's requirements because "the search warrant erroneously described the place to be searched as the server, located in Virginia" rather than Defendant's computer in the Southern District of Texas. Doc. 35 at 12. The Government responds that "[e]ven if the defendant were correct that the warrant did not fit within the letter of Rule 41(b), the use of the NIT would nevertheless still be reasonable under the Fourth Amendment." Doc. 36 at 11.

i. Probable cause[1]

In issuing a warrant, "[t]he task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). On review, the duty of the district court is "simply to ensure that the magistrate had a 'substantial basis for . . . conclud[ing]' that probable cause existed." *Id.* at 238–39 (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)). Because "[r]easonable minds frequently may differ on the question whether a particular affidavit establishes probable cause . . . the preference for warrants is most appropriately effectuated by according 'great deference' to a magistrate's determination." *United States v. Leon*, 468 U.S. 897, 914 (1984). Accordingly, the question now becomes whether, under the totality of the circumstances, it was reasonable for the magistrate judge to infer that there was a probability or substantial chance of criminal activity being committed by Playpen users and that deploying the NIT protocol onto the Playpen website in Virginia would reveal evidence of violations of federal

[1] Defendant does not appear to contest the probable-cause requirement for the warrant issued here. *See* Doc. 35. Nevertheless, the Court will address it in an abundance of caution.

law. *See Gates*, 462 U.S. at 230–31.

The affidavit on which the magistrate judge relied in this case is incredibly detailed and was provided by an agent with many years of experience. *See* Doc. 35-2. Moreover, it specifies how the TOR network operates and establishes that users of Playpen had to register for the site in order to login and download images. *Id.* The Court concludes this is sufficient to demonstrate to the issuing magistrate that there was probable cause to believe that users logged on to Playpen with the intent to engage in illegal acts. The Court's conclusion that probable cause existed to deploy the NIT against users who logged into the site and began downloading content is only bolstered by the Fifth Circuit's conclusion that mere membership in a child pornography website—even absent evidence of downloading content—provides sufficient probable cause for a search warrant. *United States v. Froman*, 355 F.3d 882, 891 (5th Cir. 2004).

ii. Particularity

The Fourth Amendment "specifies only two matters that the warrant must particularly describe: the place to be searched and the persons or things to be seized." *United States v. Grubbs*, 547 U.S. 90, 97 (2006) (internal quotation marks omitted). "The test for determining the adequacy of the description of the location to be searched is whether the description is sufficient 'to enable the executing officer to locate and identify the premises with reasonable effort, and whether there is any reasonable probability that another premise might be mistakenly searched.'" *United States v. Bonner*, 808 F.2d 864, 866 (1st Cir. 1986) (citations omitted).

Defendant contends that the warrant at issue fails the particularity requirement because it did not describe the place to be searched, i.e., Defendant's computer in Texas, and "described the information to be seized as data from the activating computers while overlooking the fact that such information could only be obtained by first searching and seizing the data from those

computers." Doc. 35 at 12. Defendant also contends that the fact that "countless other computers" were also searched only bolsters the conclusion that the search was invalid. *Id.* The Government responds that the fact "[t]hat a warrant authorizes the search of a potentially large number of suspects is an indication, not of constitutional infirmity, but a large number of criminal suspects." Doc. 36 at 14.

Again, the Court agrees with the Government. The description of the premises to be searched in this case was: "activating computer—wherever located." Doc. 35-2 at 33. This description is sufficiently particular to conclude that there is no reasonable probability that another premise might be mistakenly searched. This is because the term "activating computer" is defined narrowly to mean "those of any user or administrator who logs into [Playpen] by entering a username and password." Doc. 35-2 at 36. The description of the items to be seized is likewise clearly specified. *See id.* at 29–30, 37.

iii. Exigent circumstances

Even were the Court to conclude that both prongs of the Fourth Amendment requirement had not been met in this case, the warrant would be justified under the exigent-circumstances exception to the warrant requirement.

One exception to the warrant requirement is the presence of "exigent circumstances." *Missouri v. McNeely*, 133 S. Ct. 1552, 1575 (2013). Exigency applies when "the needs of law enforcement [are] so compelling that the warrantless search is objectively reasonable under the Fourth Amendment." *Mincey v. Arizona*, 437 U.S. 385, 393–94 (1978) (citations omitted). The Fifth Circuit considers a non-exhaustive list of factors to assess whether an exigency justifies a warrantless search:

> (1) the degree of urgency involved and the amount of time necessary to obtain a warrant;

> (2) the reasonable belief that contraband is about to be removed;
> (3) the possibility of danger to the police officers guarding the site of contraband while a search warrant is sought;
> (4) information indicating that the possessors of the contraband are aware that the police are on their trail; and
> (5) the ready destructibility of the contraband and the knowledge that efforts to dispose of narcotics and to escape are characteristic behavior of persons engaged in the narcotics traffic.

United States v. Jones, 239 F.3d 716, 720 (5th Cir. 2001) (citing *United States v. Blount*, 123 F.3d 831, 837 (5th Cir. 1997); *United States v. Rico*, 51 F.3d 495, 501 (5th Cir.1995); *United States v. Richard*, 994 F.2d 244, 248 (5th Cir. 1993)).

Here, the Government urges that the exigent-circumstances exception applies because Playpen enabled ongoing sexual abuse and exploitation of children, the information was fleeting because of the site's use of the TOR network, and the NIT warrant was minimally invasive and specifically targeted at the fleeting identifying information. Doc. 36 at 11–13. The Court agrees. First, the affidavit establishes that Playpen users were not only viewers of child pornography, but some of them were actively exploiting children by either producing pornographic content or sharing instructions with other users on how to engage in the sexual exploitation of children. *See* Doc. 35-2 at 19, 21–25. As the Government notes in its reply to Defendant's motion, after the NIT was deployed, twenty-six child victims were identified and recovered. Doc. 36 at 12. Playpen users' employment of the TOR network also indicates their intent to prevent detection of their illicit online activities. Moreover, the nature of child pornography makes it easily deletable. Because children were at immediate risk of sexual exploitation and there was a real risk that the perpetrators of these crimes would go undetected, the Court concludes that exigent circumstances existed that would justify a warrantless deployment of the NIT. *See United States v. Marvin*, 575 Fed. App'x 255, 256 (5th Cir. 2014), *cert. denied*, 135 S. Ct. 504 (2014) (per curiam) (unpublished) (concluding that immediate risk of sexual exploitation of children justified

warrantless search of defendant's residence).

c. Good-faith exception

Suppression of evidence collected pursuant to what is later determined to be an invalid warrant is not mandated when officers relied in good faith on an objectively reasonable search warrant issued by a neutral and detached judge. *Leon*, 468 U.S. at 926. The "good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Id.* at n.23. The court may consider all of the circumstances in making this determination. *Id.* However, "'a warrant issued by a magistrate normally suffices to establish' that a law enforcement officer has 'acted in good faith in conducting the search.'" *Id.* at 922 (quoting *United States v. Ross*, 456 U.S. 798, 823 n.32 (1982)). Indeed, the Supreme Court has concluded that suppression is the exception rather than the norm and should only be ordered on a case-by-case basis. *Id.* at 918. Nevertheless, the Court held that there are four circumstances in which exclusion is the appropriate remedy: (1) the issuing magistrate was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth; (2) the issuing magistrate wholly abandoned his judicial role; (3) the affidavit on which the warrant is based is so lacking in indicia of probable cause that no reasonable officer could rely on it in good faith; or (4) the warrant is facially deficient in its description of the place to be searched or thing to seized. *Id.* at 923.

Defendant alleges that "the officers acted in intentional and deliberate disregard of Rule 41," thereby precluding the Government from asserting the good-faith exception. Doc. 35 at 12–13. Specifically, Defendant argues that "there can be no credible argument that officers reasonably believed that none of the 214,898 members of [Playpen] were located outside of

Virginia." *Id.* at 13. The Government counters that the good-faith exception applies because (1) "the NIT warrant affidavit contained no knowingly or recklessly false information"; (2) Defendant does not allege that the issuing magistrate abdicated her judicial role; (3) "[t]he warrant clearly and particularly described the locations to be searched and items to be seized"; and (4) "the affidavit made a strong, comprehensive showing of probable cause." Doc. 36 at 17.

Yet again, the Court agrees with the Government. There is no indication that any of the four circumstances mandating suppression apply to this case. As already discussed, the Court is of the opinion that probable cause was established by the affidavit and the warrant sufficiently described the place to be searched. Nor is there evidence that the magistrate abdicated her role in issuing the warrant or relied on information in the affidavit that the affiant knew to be false.

d. Rule 41

The Federal Magistrates Act, 28 U.S.C. § 636(a), provides that "[e]ach United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge . . . all powers and duties conferred or imposed . . . by law or by the Rules of Criminal Procedure." Federal Rule of Criminal Procedure 41(b) confers upon the magistrate judge the authority to issue search warrants in five distinct circumstances. In this case, the parties only dispute the applicability of three of the five provisions of Federal Rule of Criminal Procedure 41. Those provisions state:

> (b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:
>
> (1) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside

> the district before the warrant is executed; . . .
>
> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and . . . .

Fed. R. Crim. P. 41.

Defendant contends that the warrant violated the Federal Magistrates Act because section 636(a) provides only three geographic areas in which a magistrate judge's powers are effective, none of which apply in this case.[2] Doc. 35 at 9. Although magistrates have authority under 41(b) to issue warrants in five circumstances, Defendant argues that none are applicable because the actual place to be searched was not the Playpen server in Virginia, but "the myriad of 'activating computers—wherever located' that would unknowingly download the NIT." *Id.* at 6. Likewise, because the property to be searched was actually Defendant's computer, which was located within the Southern District of Texas, Rule 41(b)(2) does not authorize the search because Defendant's computer was never within the Eastern District of Virginia. *Id.* at 8. Rule 41(b)(4) is also unavailing because "the NIT here was installed on the defendant's computer in Texas, which was never physically located within the Eastern District of Virginia." *Id.* In an attempt to support his arguments that the search exceeded the jurisdictional limits of Rule 41(b), Defendant contends that the "the seized server would have to send out the pornographic images with the

---

[2] The Federal Magistrates Act states in full:

> Each United States magistrate judge serving under this chapter shall have [1] within the district in which sessions are held by the court that appointed the magistrate judge, [2] at other places where that court may function, and [3] elsewhere as authorized by law . . . all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts . . . .

28 U.S.C.A. § 636.

ghost signal and its additional computer instructions, called a Network Investigative Technique ('NIT') to computers around the world, and not merely in the Eastern District of Virginia." *Id.* at 2.

In support of his plain-language arguments that Rule 41 does not support the warrant issued here, Defendant also points to a proposed amendment to Rule 41 that would expressly encompass an NIT search and was proposed specifically to address the "special difficulties" the Government encounters when investigating crimes involving electronic information. *Id.* at 13–14. This amendment would add Rule 41(b)(6), which "would authorize a court to issue a warrant to use remote access to search electronic storage media and seize electronically stored information inside or outside of the district: (1) when a suspect has used technology to conceal the location of the media to be searched." *Id.* (quoting Proposed Rule 41(b)(6)).

The Government responds that "[s]ection 636(a) limits where a magistrate may *possess* his powers, but not where those powers can have *effect*" and "Rule 41(b) supports this reading that a magistrate can possess a power that has effects beyond the places described in Section 636(a)." Doc. 36 at 11. The Government also disagrees with Defendants' characterization of how the NIT operated, arguing that the search at issue falls squarely within all three relevant provisions of Rule 41. *Id.* at 7–10. First, the Government argues 41(b)(1) applies because Defendant actually entered the Eastern District of Virginia, albeit not physically, by accessing the Playpen server there. *Id.* at 8. He then retrieved the NIT from that server, and the NIT sent his network information back to a server in that district. *Id.* The Government's next argument is that 41(b)(2) applies because Rule 41(a)(2)(A) defines "property" to include both "tangible objects" and "information." *Id.* at 7. Under this definition, the NIT constitutes the property. *Id.* Because this property was located within the Eastern District of Virginia when the warrant was

issued and the NIT was deployed only to registered users of the website, each of those users "reached into the Eastern District of Virginia's jurisdiction to access the site." *Id.* "Thus, Rule 41(b)(2) provided sufficient authority to issue the warrant for use of the NIT even outside of the Eastern District of Virginia." *Id.* at 8. Finally, the Government argues that Rule 41(b)(4) provides authority for the warrant because the NIT acted like a "tracking device," which is defined to be "an electronic or mechanical device which permits the tracking of the movement of a person or object." *Id.* (quoting Rule 41(a)(2)(E); 18 U.S.C. § 3117(b)). This argument rests on the fact that the NIT was installed within the Eastern District of Virginia and was only retrieved when Defendant logged into the server that hosted Playpen. *Id.* The NIT then "attached" and sent network information from Defendant's computer back to law enforcement. *Id.* The Government also contests Defendants' explanation of the purpose of the proposed amendment to Rule 41. *Id.* at 10. It argues that rather than "authoriz[ing] the government to undertake a search or seizure, or use any remote search technique not already permitted under current law," the amendment was simply designed to clarify that courts have venue to issue a warrant in such circumstances. *Id.*

The Court agrees with the Government that Rule 41(b) provides ample authority for the warrant in this case. Unlike Defendant suggests, the server did not send out unsolicited pornographic images willy-nilly to computers all over the globe. Rather, the NIT was installed on the server in the Eastern District of Virginia, where both the server and NIT sat passively until an individual sought to avail himself of Playpen's known pornographic content. Indeed, in order for the NIT to "attach," an individual seeking to obtain prohibited content had to navigate to the Playpen website using its distinct URL, login with a username and password that he had registered for, view a menu of images, and then click on what he wanted to download. It was only then that the NIT would download from the server. Only once "attached" through

Defendant's actions (after he entered the Eastern District of Virginia via the Internet) would the NIT then prompt his home computer to share its IP address. These facts about how the NIT functioned are more than enough to convince the Court that the warrant was justified, at the very least, under Rule 41(b)(4). Moreover, Defendants' reliance on the proposed amendment to Rule 41 is misplaced. As the Government points out, the proposed amendment and accompanying memorandum actually support the Government's contention that the amendment seeks only to clarify the Rule—not expand its scope. One DOJ memorandum clearly states:

> As we have stated previously, the proposed amendment would ensure that a court has jurisdiction to issue a search warrant in two categories of investigations involving modern Internet crime: cases involving botnets and cases involving Internet anonymizing techniques. The proposal would do so by clarifying Rule 41's current venue provisions in these two circumstances. The proposal would not authorize the government to undertake any search or seizure or use any remote search technique not already permitted under current law.

Advisory Committee on Criminal Rules, *DOJ's Response to Comments Concerning Proposed Amendment to Rule 41* 139 (Dec. 22, 2014), available at:

file:///C:/Users/mh_lc3/Downloads/CR2015-05.pdf.

Finally, the Court notes that although none are binding on this Court, it is extremely persuasive that the vast majority of our sister districts to have considered motions to suppress in the context of the deployment of the NIT to identify Playpen users have reached the same outcome as the Court does today by relying on one of the Government's aforementioned arguments. *See United States v. Jean*, 5:15-CR-50087-001, 2016 WL 4771096, at *15 (W.D. Ark. Sept. 13, 2016) (collecting and describing each of the Playpen motion-to-suppress opinions and stating that only two of them "went so far as to suppress the evidence.").

IV. Conclusion

For the foregoing reasons, it is hereby

ORDERED that Defendant's Motion to Suppress Evidence Under Seal, Doc. 35, is **DENIED**.

SIGNED at Houston, Texas, this 28th day of September, 2016.

MELINDA HARMON
UNITED STATES DISTRICT JUDGE